

Федерации такого рода сбор и хранение информации, полученной операторами связи, приведут лишь к избыточной нагрузке обеспечивающей инфраструктуры провайдеров связи, а не к достижению основной заявленной цели (указанной выше).

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ ЗАЩИТЫ ОБЪЕКТОВ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ И ТРАНСПОРТНЫХ СРЕДСТВ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

М. М. Лысых, Т. Ю. Зырянова
(Екатеринбург, УрГУПС)

Обеспечение транспортной безопасности – это одно из направлений стратегии развития транспортного комплекса Уральского региона до 2030 г.

В соответствии с Федеральным законом «О транспортной безопасности» № 16 от 09.02.2007 г. [1] обеспечение транспортной безопасности – это реализация определяемой государством системы правовых, экономических, организационных и иных мер в сфере транспортного комплекса, соответствующих угрозам совершения актов незаконного вмешательства.

Целями обеспечения транспортной безопасности являются устойчивое и безопасное функционирование транспортного комплекса, защита интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Акт незаконного вмешательства (далее АНВ) – противоправное действие (бездействие), в том числе террористический акт, угрожающее безопасной деятельности транспортного комплекса, повлекшее за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшее угрозу наступления таких последствий.

Требования по обеспечению транспортной безопасности, согласно ст. 8 вышеупомянутого закона, являются обязательными для исполнения всеми субъектами транспортной инфраструктуры.

Требования по обеспечению транспортной безопасности, учитывающие уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта, утверждены приказом Минтранса РФ от 08.02.2011 г. № 43 [2].

Требования определяют систему мер, реализуемых субъектами транспортной инфраструктуры, для защиты объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта (далее ОТИ и ТС) от потенциальных, непосредственных и прямых угроз совершения актов незаконного вмешательства.

Согласно п. 3 ст. 12 «Права и обязанности субъектов транспортной инфраструктуры и перевозчиков в области обеспечения транспортной безопасности» субъекты транспортной инфраструктуры и перевозчики несут ответственность за неисполнение требований по обеспечению транспортной безопасности в соответствии с законодательством Российской Федерации.

Ниже приведены основные изменения в области транспортной безопасности.

Издан приказ Министерства транспорта России от 11.02.2010 г. № 34 «Об утверждении порядка разработки планов обеспечения транспортной безопасности объектов транспортной инфраструктуры и транспортных средств» [3].

Издан приказ Минтранса России № 52, ФСБ России № 112, МВД России № 134 от 05.03.2010 г. «Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств» [4].

Указ Президента РФ от 31.03.2010 г. № 403 «О создании комплексной системы обеспечения безопасности населения на транспорте» определил Министерство транспорта Российской Федерации в качестве федерального органа исполнительной власти, ответственного за создание комплексной системы обеспечения безопасности населения на транспорте, прежде всего на метрополитене и других видах общественного транспорта, предотвращения чрезвычайных ситуаций и террористических актов на транспорте, а также обеспечения защиты населения [5].

Издан приказ Министерства транспорта России от 12.04.2010 г. № 87 «О порядке проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств» [6].

Приказ Министерства транспорта России от 26.07.2011 г. № 199 «О внесении изменения в приказ Министерства транспорта России от 12.04.2010 г. № 87» исключил необходимость использования методик для проведения оценки уязвимости [7].

Издан приказ Министерства транспорта России от 08.02.2011 г. № 43 «Об утверждении требований по обеспечению транспортной безопасности, учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта».

Издан приказ Росжелдора от 25.10.2011 г. № 515 «Об утверждении методических рекомендаций по проведению оценки уязвимости объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта». Методические рекомендации по проведению оценки уязвимости объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта (далее Методические рекомендации) рекомендуют к применению общие положения для проведения оценки уязвимости объектов транспортной инфраструктуры (далее ОТИ) и транспортных средств (далее ТС) железнодорожного транспорта. Методические рекомендации предназначены для использования специализированными организациями при проведении оценки уязвимости ОТИ и ТС.

Приказ Министерства транспорта России от 07.03.2013 г. № 73 «Об отмене приказа Росжелдора от 25.10.2011 г. № 515 “Об утверждении методических рекомендаций по проведению оценки уязвимости объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта”» признал утратившими силу методические рекомендации [8]. Методика была отменена по причине того, что в оценке уязвимости не уделялось должного внимания информационной составляющей ОТИ. Уязвимости в сфере информационных технологий не рассматривались.

Сравнительные показатели актов незаконного вмешательства в работу Свердловской железной дороги приведены в следующей таблице:

Год	Количество АНВ за первые 9 месяцев	Ущерб за первые 9 месяцев, млн руб.
2011	1 147	12,5
2012	924	15,7
2013	561	11

Несмотря на принятые меры защиты и соблюдение всех необходимых требований по обеспечению транспортной безопасности, АНВ происходят, но уже в меньшем количестве, что свидетельствует о правильности применяемых методов. Величина ущерба зависит от количества АНВ. Для построения более гибкой системы организации транспортной безопасности целесообразно использовать методы математического моделирования. После создания некоторой математической модели уязвимости элемента или объекта транспортной инфраструктуры появляется возможность прогнозировать вероятный размер ущерба, а также рассмотреть целесообразность модернизации системы для снижения вероятности появления события АНВ и минимизации итогового ущерба.

Библиографические ссылки

1. О транспортной безопасности: ФЗ от 09.02.2007 г. № 16-ФЗ.
2. Об утверждении требований по обеспечению транспортной безопасности, учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта : приказ Министерства транспорта России от 08.02.2011 г. № 43.
3. Об утверждении порядка разработки планов обеспечения транспортной безопасности объектов транспортной инфраструктуры и транспортных средств : приказ Министерства транспорта России от 11.02.2010 г. № 34.
4. Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств : приказ Минтранса России № 52, ФСБ России № 112, МВД России № 134 от 05.03.2010 г.
5. О создании комплексной системы обеспечения безопасности населения на транспорте : Указ Президента РФ от 31.03.2010 г. № 403.

6. О порядке проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств : приказ Министерства транспорта России от 12.04.2010 г. № 87.

7. О внесении изменения в приказ Министерства транспорта России от 12.04.2010 г. № 87 : приказ Министерства транспорта России от 26.07.2011 г. № 199.

8. Об отмене приказа Росжелдора от 25.10.2011 № 515 : приказ Министерства транспорта России от 7.03.2013 г. № 73.

ОСОБЕННОСТИ ТРЕБОВАНИЙ РОСКОМНАДЗОРА К ОПЕРАТОРАМ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПРОВЕДЕНИИ ПЛАНОВЫХ ВЫЕЗДНЫХ ПРОВЕРОК В СУБЪЕКТАХ РОССИЙСКОЙ ФЕДЕРАЦИИ

Е. Л. Рублев

(Челябинск, ЮУрГУ (национальный исследовательский университет),
rublev16@mail.ru)

Введение

Законодательство в сфере персональных данных постоянно подвергается различного рода изменениям. В таких условиях операторам сложно следить за изменениями в законодательстве и регулярно вносить корректировки в документацию по защите персональных данных. В случае, если в организации отсутствует отдел защиты информации (отдел информационной безопасности) или штатный сотрудник, занимающийся непосредственно защитой информации, следить за изменениями в законодательстве и дорабатывать локальную документацию невозможно.

К проверке оператора на соблюдение требований по защите персональных данных со стороны регулирующего органа – Роскомнадзора – сложно подготовиться сотруднику, который не является профессионалом в области защиты информации. К тому же в зависимости от субъекта Российской Федерации требования, которые предъявляет регулятор, отличаются между собой. Ни в одном нормативно-правовом акте нет полного, исчерпывающего списка до-